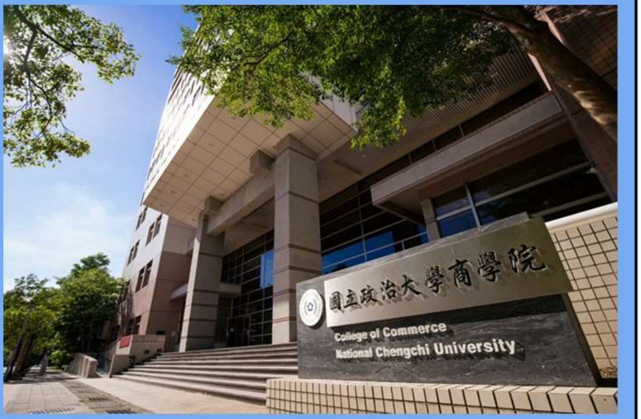
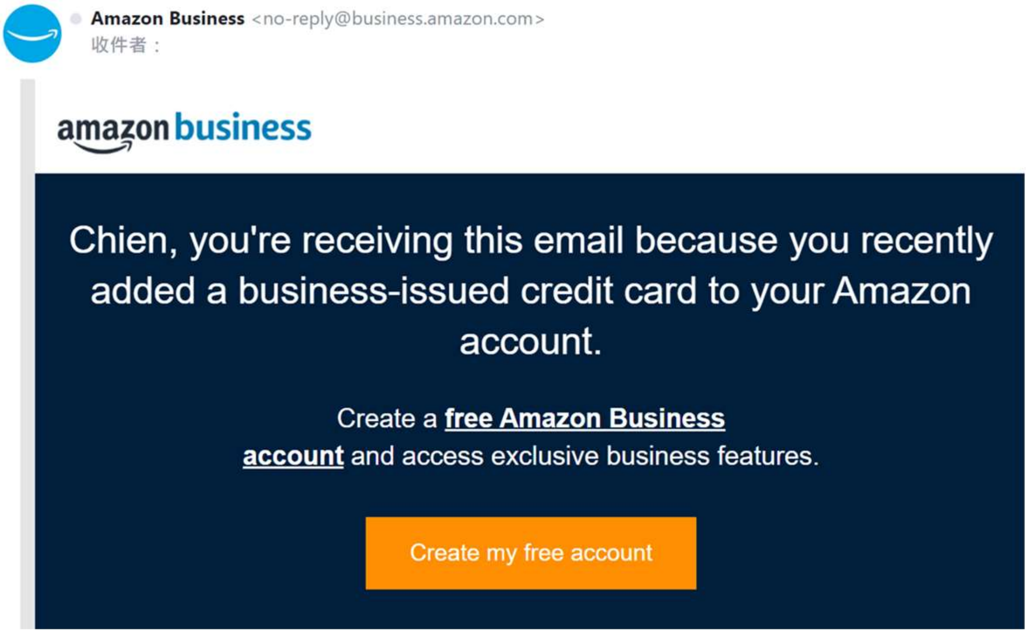
國立政治大學資訊管理學系
NCCU DEPARTMENT OF MANAGEMENT INFORMATION SYSTEMS

Introduction to Computer Science

Week 6- Digital Security and Privacy Security



Shih-Yi (James) Chien
Assistant Professor
Dept. of Management Information Systems
Email: sychien@nccu.edu.tw

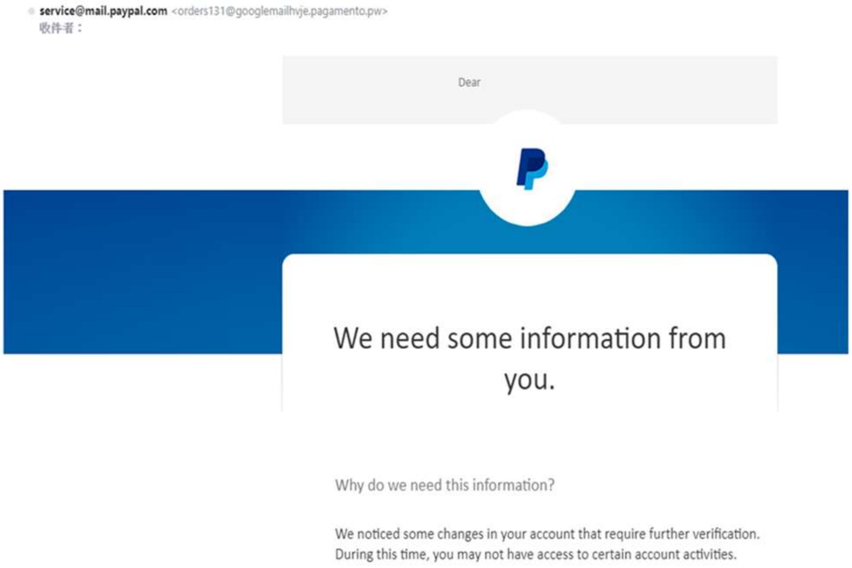


Amazon Business <no-reply@business.amazon.com>
收件者：

amazon business

Chien, you're receiving this email because you recently added a business-issued credit card to your Amazon account.

Create a **free Amazon Business account** and access exclusive business features.



service@mail.paypal.com <orders131@googlemailhvje.pagamento.pw>
收件者：

Dear

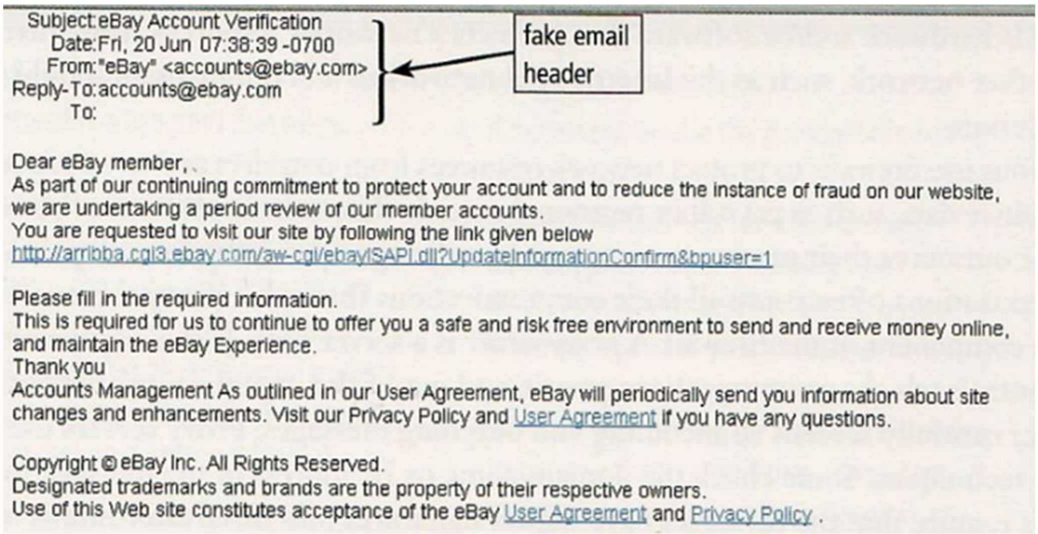
We need some information from you.

Why do we need this information?

We noticed some changes in your account that require further verification. During this time, you may not have access to certain account activities.

Email Spoofing

spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust



Subject:eBay Account Verification
Date:Fri, 20 Jun 07:38:39 -0700
From:"eBay" <accounts@ebay.com>
Reply-To:accounts@ebay.com
To:

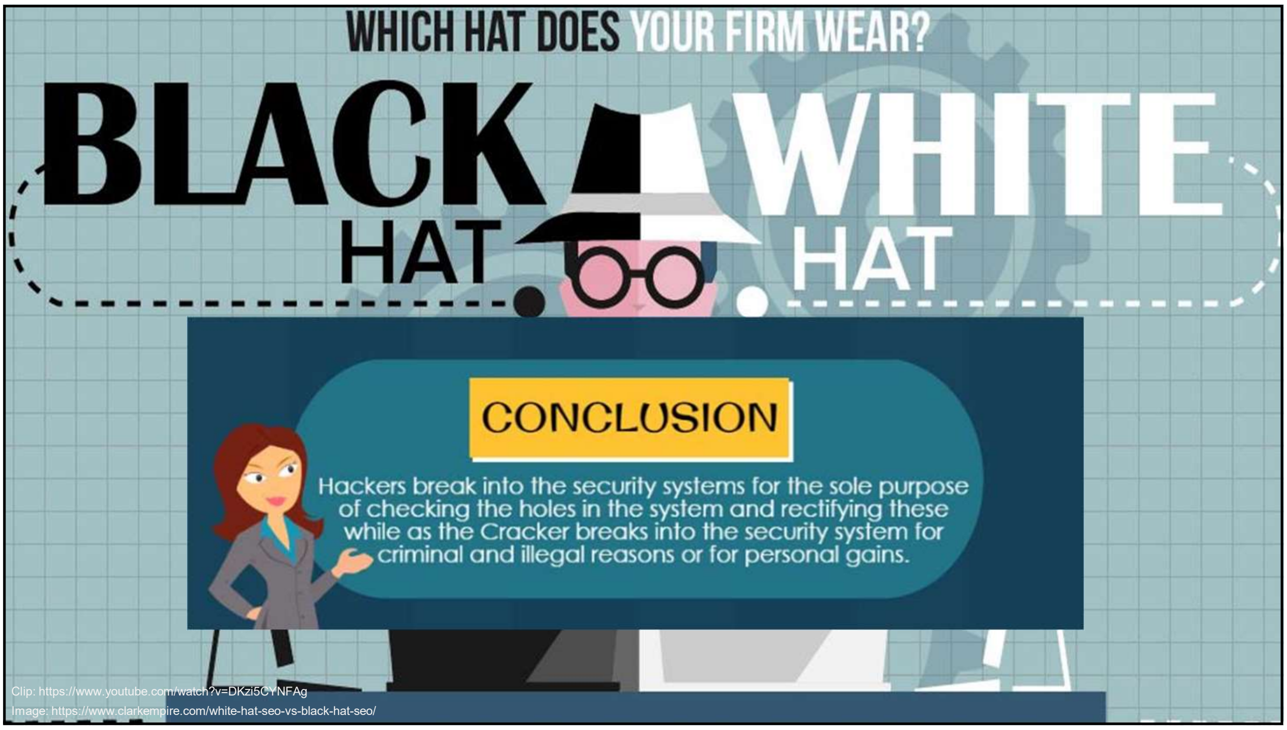
fake email header

Dear eBay member,

As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.
You are requested to visit our site by following the link given below
http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1

Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy .

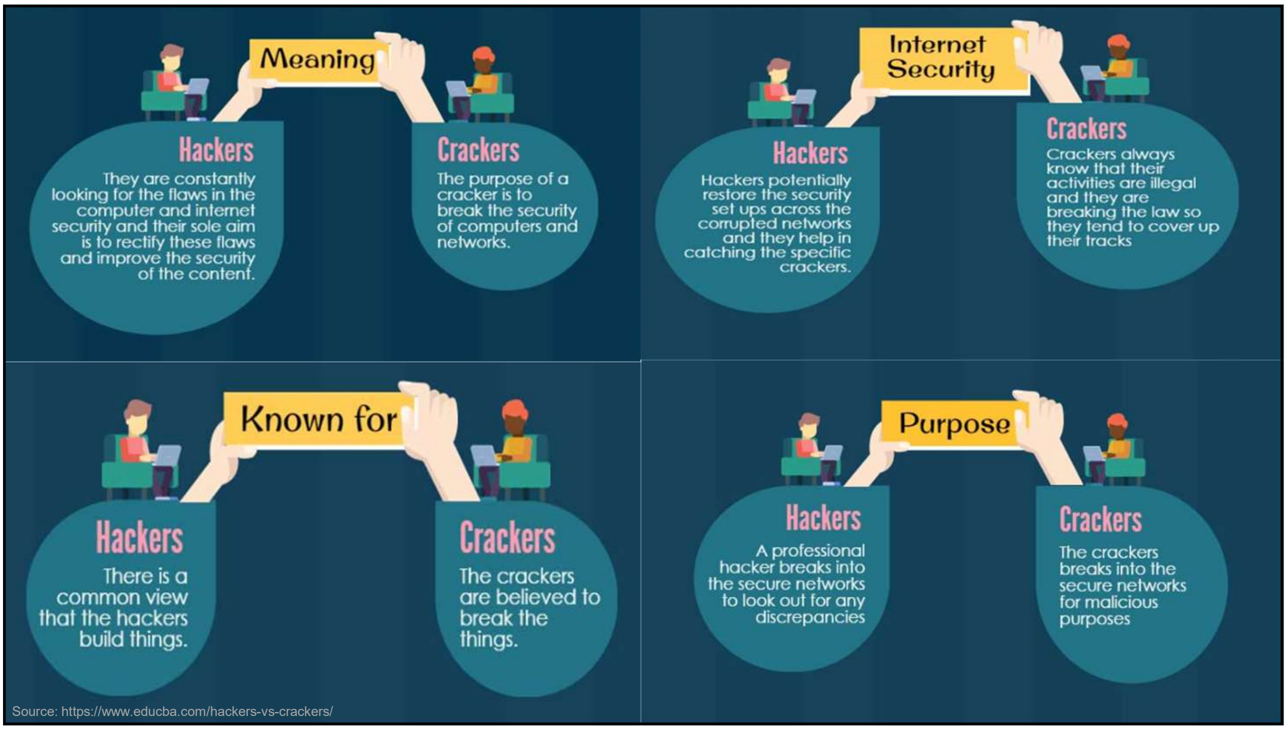


CONCLUSION

Hackers break into the security systems for the sole purpose of checking the holes in the system and rectifying these while as the Cracker breaks into the security system for criminal and illegal reasons or for personal gains.

Clip: https://www.youtube.com/watch?v=DKzi5CYNFAg

Image: https://www.clarkempire.com/white-hat-seo-vs-black-hat-seo/



Meaning

Hackers: They are constantly looking for the flaws in the computer and internet security and their sole aim is to rectify these flaws and improve the security of the content.

Crackers: The purpose of a cracker is to break the security of computers and networks.

Internet Security

Hackers: Hackers potentially restore the security set ups across the corrupted networks and they help in catching the specific crackers.

Crackers: Crackers always know that their activities are illegal and they are breaking the law so they tend to cover up their tracks

Known for

Hackers: There is a common view that the hackers build things.

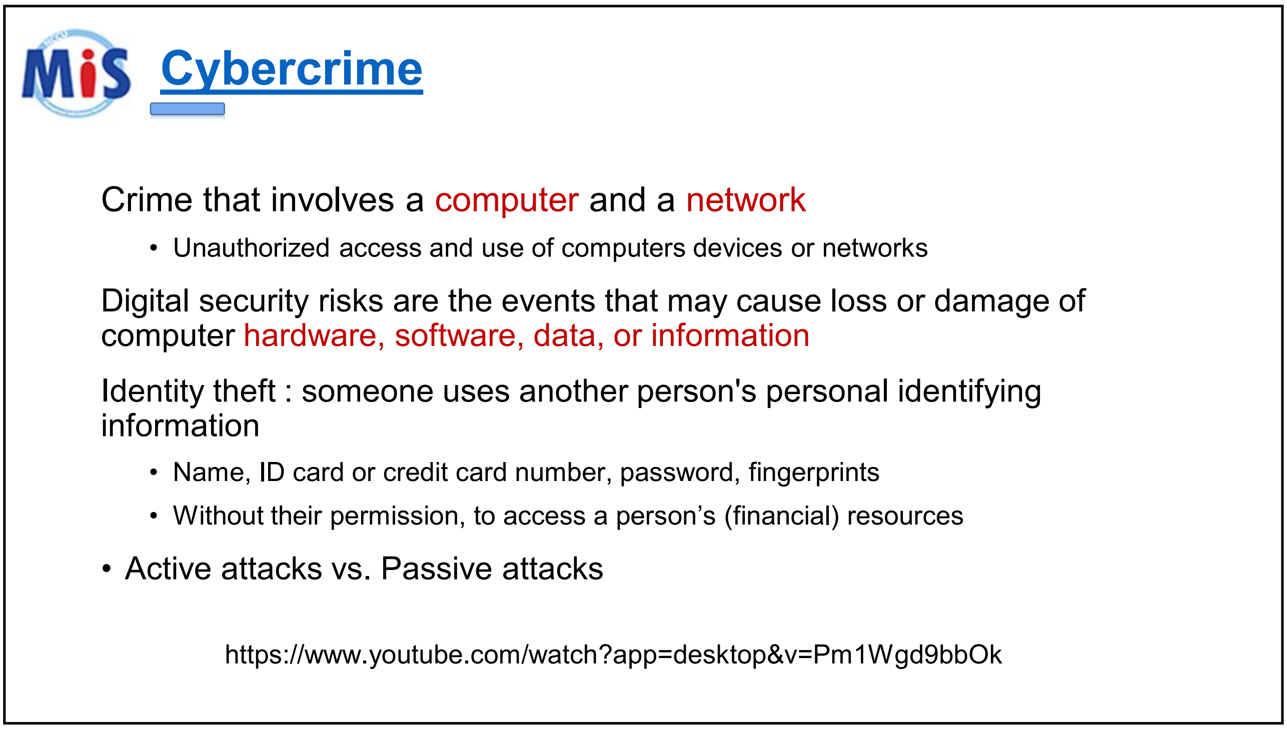
Crackers: The crackers are believed to break the things.

Purpose

Hackers: A professional hacker breaks into the secure networks to look out for any discrepancies

Crackers: The crackers breaks into the secure networks for malicious purposes

Source: https://www.educba.com/hackers-vs-crackers/



Cybercrime

Crime that involves a computer and a network

- Unauthorized access and use of computers devices or networks

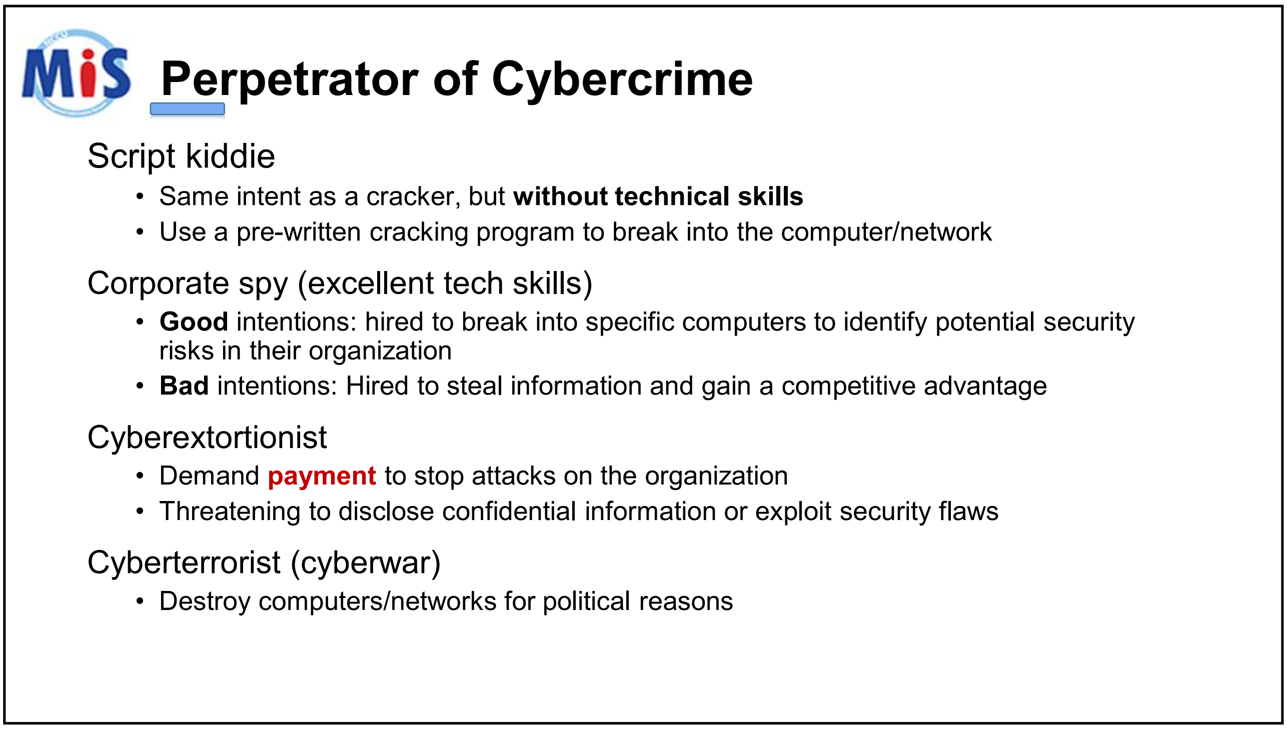
Digital security risks are the events that may cause loss or damage of computer hardware, software, data, or information

Identity theft : someone uses another person's personal identifying information

- Name, ID card or credit card number, password, fingerprints
- Without their permission, to access a person’s (financial) resources

- Active attacks vs. Passive attacks

https://www.youtube.com/watch?app=desktop&v=Pm1Wgd9bbOk



Perpetrator of Cybercrime

Script kiddie

- Same intent as a cracker, but **without technical skills**
- Use a pre-written cracking program to break into the computer/network

Corporate spy (excellent tech skills)

- **Good** intentions: hired to break into specific computers to identify potential security risks in their organization
- **Bad** intentions: Hired to steal information and gain a competitive advantage

Cyberextortionist

- Demand **payment** to stop attacks on the organization
- Threatening to disclose confidential information or exploit security flaws

Cyberterrorist (cyberwar)

- Destroy computers/networks for political reasons

Malware

Malware (malicious software) is run by programs that run without the user’s knowledge and deliberately change the operation of computers and mobile devices

- Social media websites
- e-commerce websites
  - Email
  - ID & Password

Source: https://en.wikipedia.org/wiki/Malware

Type	Description
Virus	Virus is a type of computer program. When executed, it replicates itself by modifying other computer programs and inserting its own code.
Ransomware	Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
Rootkit	allows an unauthorized user to have privileged access to a computer and to restricted areas of its software. A rootkit may contain a number of malicious tools such as keyloggers, banking credential stealers, password stealers.
Spyware	To gather information about a person or organization and send such information to another entity in a way that harms the user; for example by violating their privacy or endangering their device's security.
Trojan horse	Spreading by some social engineering. A user executes an email attachment disguised to appear not suspicious, or by clicking on some fake advertisement on social media or anywhere else.
Adware	Generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process.
Worm	A computer worm is a standalone malware computer program that **replicates itself** in order to spread to other computers. By using this machine as a host to scan and infect other computers, it often uses a computer network to spread itself.

Back Door Attacks

Back door is a program that allows users to bypass the security control program and remotely access the computer without the user's knowledge

- Programmers often install back doors to test programs

Botnet is a group of compromised (mobile) computers connected to the network

- A compromised computer or device is called as a **zombie**
- The owner does not know that the computer is remotely controlled by an outsider

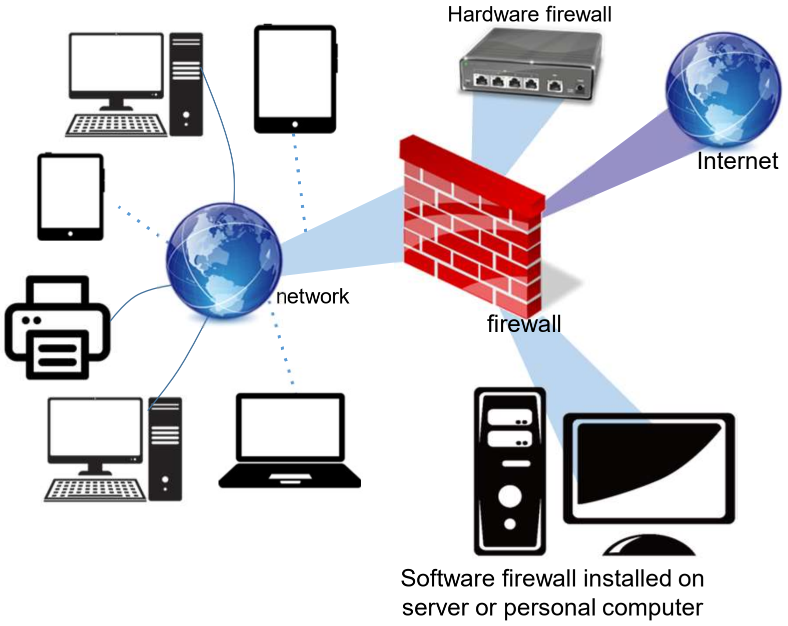
Denial of service attack (**DoS attack**) disrupts computer access to Internet

- Distributed DoS attack (DDoS attack)

Clip: https://www.youtube.com/watch?v=c9EjuOQRUdg

Firewall

Firewall is hardware and/or software that protects a network's resources from intrusion



Hardware firewall

Internet

network

firewall

Software firewall installed on server or personal computer

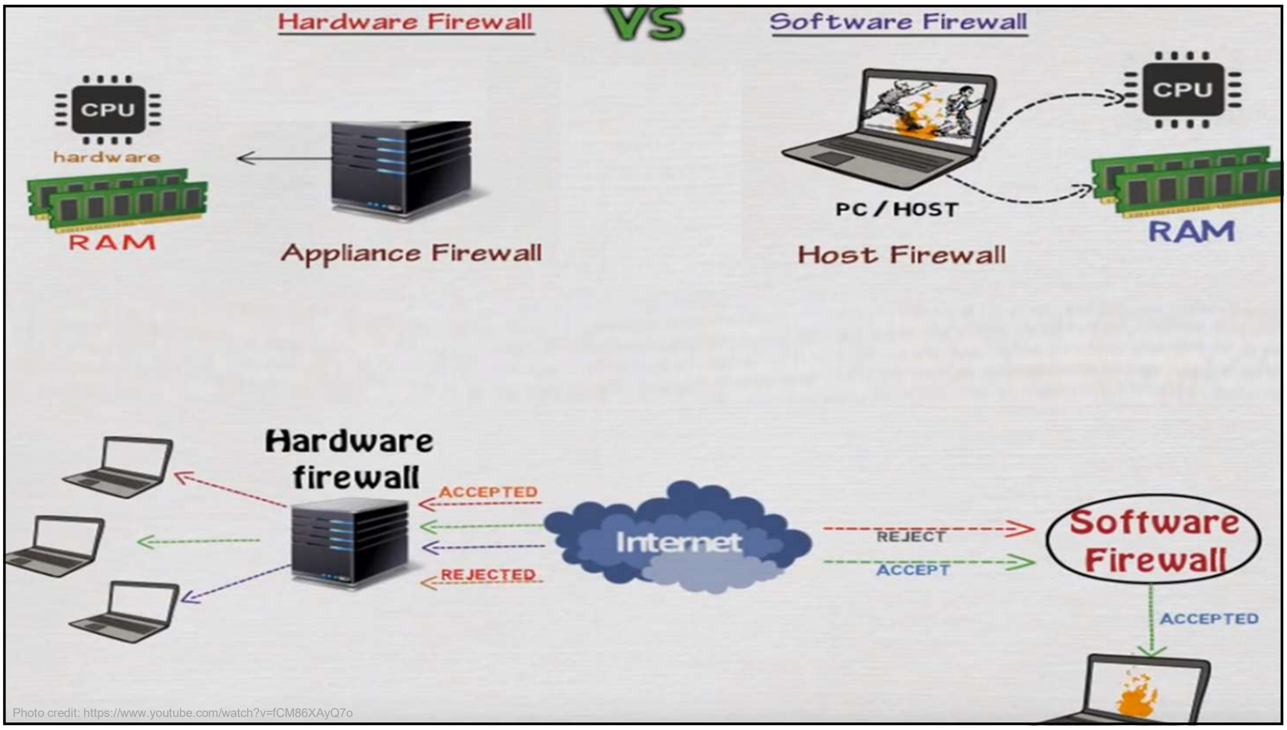
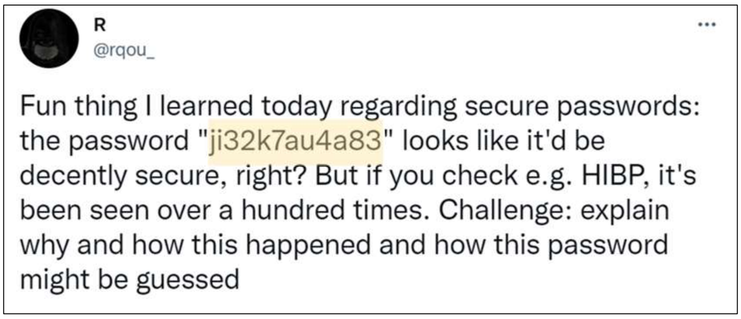


Photo credit: https://www.youtube.com/watch?v=fCM86XAyQ7o

Worst Passwords of 2022

1	123456
2	123456789
3	qwerty
4	password
5	12345
6	12345678
7	111111
8	1234567
9	123123
10	qwerty123
11	1q2w3e
12	1234567890
13	DEFAULT
14	000000
15	abc123



R
@rqou_

Fun thing I learned today regarding secure passwords: the password "ji32k7au4a83" looks like it'd be decently secure, right? But if you check e.g. HIBP, it's been seen over a hundred times. Challenge: explain why and how this happened and how this password might be guessed

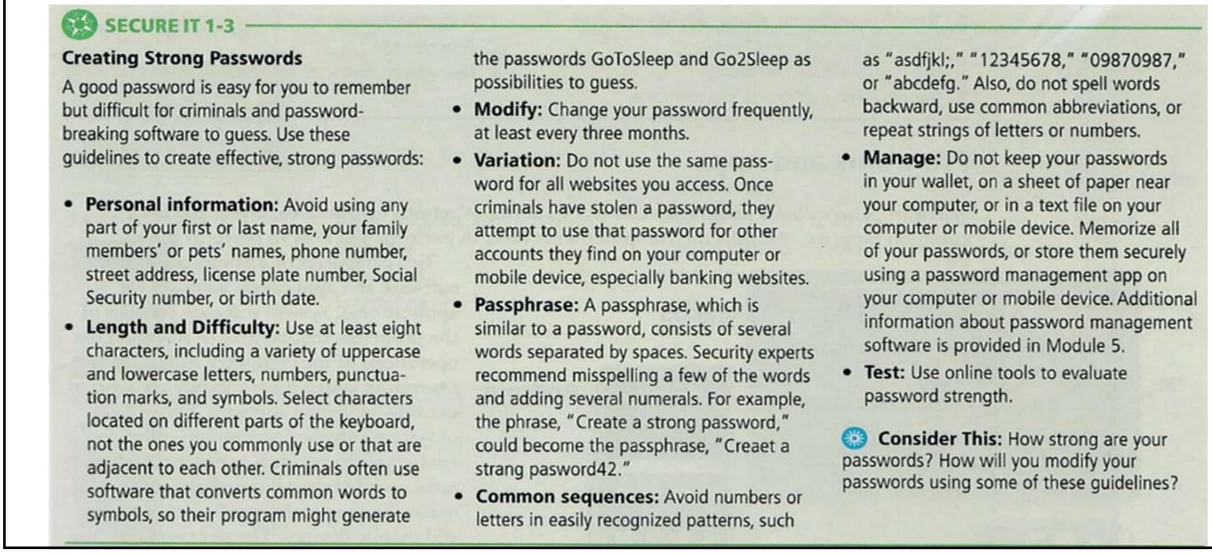
au4a83 密碼

ji32k7au4a83 我的密碼

Source: https://www.tomsguide.com/news/worst-passwords-2022

Creating Strong passwords

- https://www.betterbuys.com/estimating-password-cracking-times/



SECURE IT 1-3

Creating Strong Passwords

A good password is easy for you to remember but difficult for criminals and password-breaking software to guess. Use these guidelines to create effective, strong passwords:

- **Personal information:** Avoid using any part of your first or last name, your family members' or pets' names, phone number, street address, license plate number, Social Security number, or birth date.
- **Length and Difficulty:** Use at least eight characters, including a variety of uppercase and lowercase letters, numbers, punctuation marks, and symbols. Select characters located on different parts of the keyboard, not the ones you commonly use or that are adjacent to each other. Criminals often use software that converts common words to symbols, so their program might generate the passwords GoToSleep and Go2Sleep as possibilities to guess.
- **Modify:** Change your password frequently, at least every three months.
- **Variation:** Do not use the same password for all websites you access. Once criminals have stolen a password, they attempt to use that password for other accounts they find on your computer or mobile device, especially banking websites.
- **Passphrase:** A passphrase, which is similar to a password, consists of several words separated by spaces. Security experts recommend misspelling a few of the words and adding several numerals. For example, the phrase, "Create a strong password," could become the passphrase, "Creaet a strang pasword42."
- **Common sequences:** Avoid numbers or letters in easily recognized patterns, such as "asdfjkl;," "12345678," "09870987," or "abcdefg." Also, do not spell words backward, use common abbreviations, or repeat strings of letters or numbers.
- **Manage:** Do not keep your passwords in your wallet, on a sheet of paper near your computer, or in a text file on your computer or mobile device. Memorize all of your passwords, or store them securely using a password management app on your computer or mobile device. Additional information about password management software is provided in Module 5.
- **Test:** Use online tools to evaluate password strength.

Consider This: How strong are your passwords? How will you modify your passwords using some of these guidelines?

Biometric Device

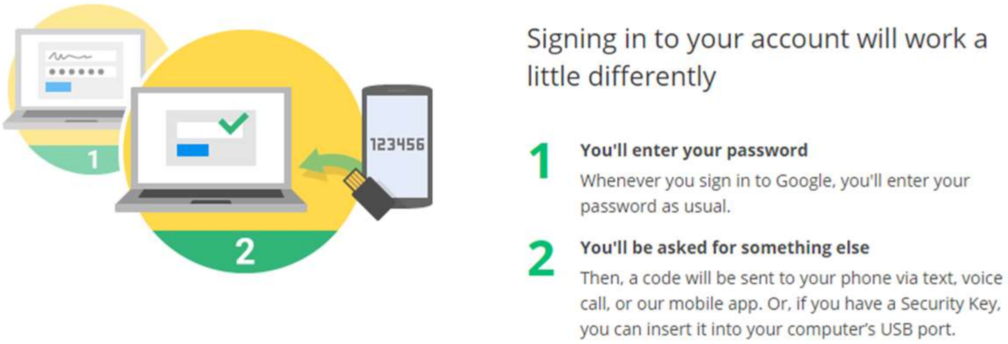
Biometric device verifies the identity of a person by converting personal characteristics into a digital code

- Fingerprint reader
- Face, voice, and signature recognition system
- Hand geometry system: shape and size
- Iris recognition system: patterns in the iris of the eye

Two-step Verification

Two-step verification uses two different methods (one after another) to verify the user's identity

- ATM card, then enter a PIN
- ID and password, then enter security code (text message)



Signing in to your account will work a little differently

1 **You'll enter your password**
Whenever you sign in to Google, you'll enter your password as usual.

2 **You'll be asked for something else**
Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.

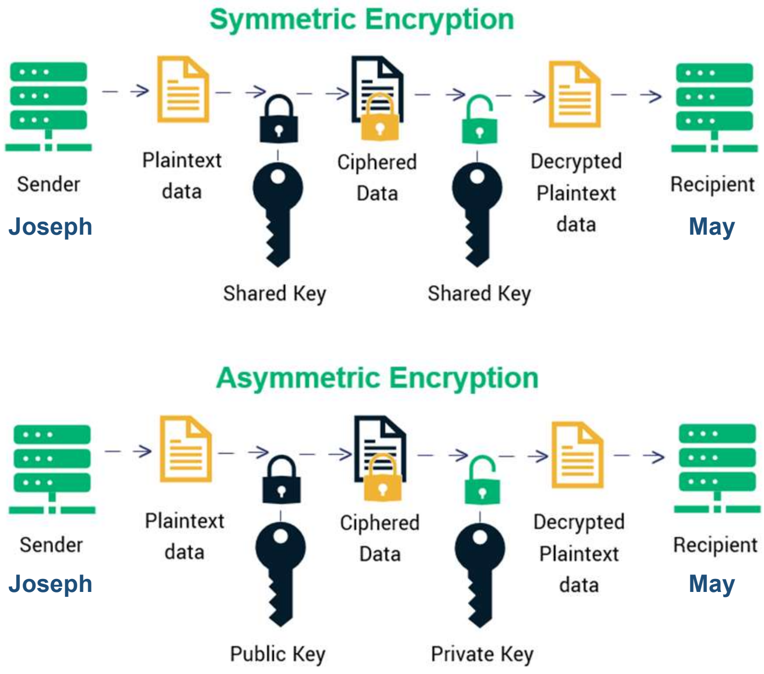
Image credit: https://www.google.com/landing/2step/#tab=how-it-

Encryption

Information theft occurs when someone steals personal or confidential information

To prevent information theft, **encryption** is the process of converting human-readable data into encoded characters to prevent unauthorized access

- To read the data, the recipient must **Decrypt**
  - Imitation Game message decoded
  - http://www.youtube.com/watch?v=_C25CwNIVjA&t=3m5s



May's public key
Joseph's private key

Joseph's public key
May's private key

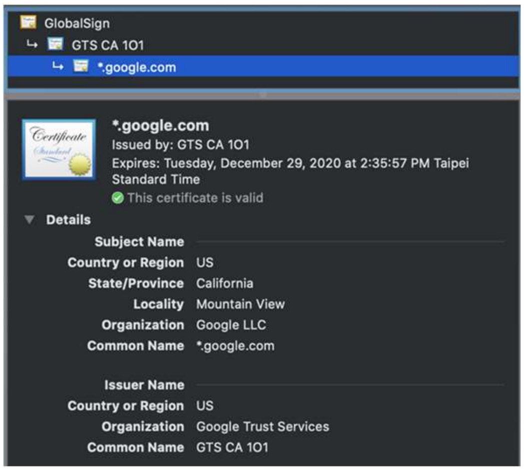
Image: sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/

Digital Signature

Digital signature is an electronic, encrypted stamp of authentication on digital information

- Integrity: ensure the info originated from the signer and was not altered; any change made to the signed data invalidates the whole signature
- Nonrepudiation: enables you to prove to have received or sent a message from or to a trading partner

Digital certificate is a notice that **guarantees** a user or a website is legitimate



GlobalSign
↳ GTS CA 1O1
↳ *.google.com

*.google.com
Issued by: GTS CA 1O1
Expires: Tuesday, December 29, 2020 at 2:35:57 PM Taipei Standard Time
✓ This certificate is valid

▼ Details

Subject Name	
Country or Region	US
State/Province	California
Locality	Mountain View
Organization	Google LLC
Common Name	*.google.com
Issuer Name	
Country or Region	US
Organization	Google Trust Services
Common Name	GTS CA 1O1